

IN THE SPECIFICATION:

Please amend the specification as follows.

[0007] NDMP was designed to allow data transfer operations over IP networks. In particular, NDMP is used for backing up heterogeneous file servers to tape drives over IP networks. ~~Because NDMP was designed for use in IP networks, it makes use of IP addresses. IP addresses, however, may change. A host device's IP address therefore cannot be used as a means for persistent identification of that device.~~ One of the features of NDMP is to allow for the possibility of changing IP addresses. Consequently, in an NDMP environment, mapping of devices (e.g., for control of access to storage devices) ~~cannot be~~ is not typically based upon the devices' IP addresses. Another mechanism ~~must~~ should therefore be provided for identifying the devices for the purpose of access control.

[0013] The various embodiments of the invention may provide a number of advantages over prior art systems and methods. For example, systems that use NDMP over an IP network to perform backup operations ~~do need~~ not provide unique worldwide names for devices on the network. ~~Instead, the devices have IP addresses that can change from time to time. As a result, no unique identification of the devices is provided to support access controls from the devices to storage devices on the network.~~ Embodiments To comport with NDMP protocol in an IP network environment, embodiments of the present invention utilize login information such as usernames and corresponding passwords to uniquely identify the devices, thereby enabling identification of the devices for the purpose of controlling access to storage devices in an NDMP IP network environment. Embodiments of the present invention also provide a unique mechanism for controlling access by maintaining tables with which the devices are associated, wherein each device can access the storage devices identified in the associated table. Various other advantages may also be provided.

[0025] In this embodiment, the router is configured to maintain one or more tables that map users to sets of the tape drives. These tables are used to control the users' access to the tape drives. Each user is uniquely identified, and this identification is used to associate the user with one of the tables, thereby allowing the user to access the tape drives listed in the table. Because NDMP does not create unique names for the devices

that are on the IP network ~~(and because the IP addresses of the devices on the network may change,~~ a mechanism is provided for assigning unique names to the users. In this embodiment, the unique names comprise usernames and corresponding passwords with which the users log onto the network.

[0032] One of the problems with NDMP-based backup systems, however, is that implementing access controls for backups may be more difficult than in other types of systems.

Consider, for example, the problem of identifying a particular device and the corresponding permissions to backup data to certain storage devices. In a Fibre Channel-based system, a first device (e.g., a file server) which is to be backed up has a unique worldwide name. Access controls can be implemented by associating this unique worldwide name with a storage device (or set of storage devices) to which the first device may backup its data. In an NDMP system, however, the network is an IP network. ~~In an IP network, devices are identified by their corresponding IP addresses. These IP addresses may change from time to time, so they~~ NDMP does not typically provide for access controls based on IP addresses. Therefore another mechanism, cannot should be used as identifiers for the purpose of implementing access controls in an NDMP IP network environment. Similarly Also, it is not always possible to use the physical (MAC) address of the devices for the purpose of uniquely identifying them. Some Embodiments of the present invention provide an alternative mechanism for uniquely identifying the devices to be backed up is therefore necessary for an NDMP IP network environment.

[0050] While the embodiments of the invention which are described above focus on an implementation in which a router positioned between one or more file servers on an IP network and one or more tape drives on a SCSI bus, the invention is contemplated to be more broadly applicable. ~~For example, some embodiments of the invention may in connection with networks that are not IP based, but which fail to provide a unique worldwide identifier of user devices and therefore require a username password identifier or similar mechanism for providing unique identification of these devices. The~~ For example, the user devices themselves also need not be limited to file servers, but may comprise any type of device that needs to access the devices to which access is controlled. Similarly, the controlled access devices need not be limited to tape drives, and need not be coupled to a SCSI bus.